Organization for Security and Co-operation in Europe

Non-paper on OSCE activities regarding implementation of cyber/ICT security confidence-building measures

For the attention of the Chairs of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security and the Group of Governmental Experts on advancing responsible state behaviour in cyberspace in the context of international security

Background

The Organisation for Security and Co-operation in Europe (OSCE) started to work on cyber/ICT security issues in 2012 and has **adopted two sets of cyber/ICT security confidence-building measures (CBM) to reduce the risks of conflict stemming from the use of information and communication technologies.** They are designed to make cyberspace more predictable and offer concrete tools and mechanisms to avoid misunderstandings, including:

- A mechanism to bring together states for consultations over potential cyber/ICT security incidents to de-escalate rising tensions;
- A platform for exchanging views, national cyber/ICT security policies and approaches to allow states to better "read" each other's intentions in cyberspace; and
- Concrete work items, for instance to protect ICT-enabled critical infrastructure, allowing participating States to collectively enhance cyber resilience in the OSCE region for the benefit of all.

The OSCE cyber/ICT security CBMs

The OSCE Permanent Council adopted the first set of **OSCE cyber/ICT CBMs** in 2013[1], the same year the UN GGE developed recommendations for confidence-building measures, while the second set was approved in 2016[2] bringing the **total number of such measures to 16**. These are **non-binding, voluntary measures**, but all the 57 OSCE participating States made a **political commitment** to adhere to them. The aim of the confidence-building measures is to **enhance interstate co-operation, transparency, predictability, and stability**, as well as to **reduce the risks of misperception, escalation, and conflict that may stem from the use of ICTs**.

The Decision on OSCE CBMs specifically mentions the United Nations by "confirming that the CBMs being elaborated in the OSCE **complement UN efforts to promote CBMs** in the field of security of and in the use of ICTs. The efforts of the OSCE participating States in implementation of the OSCE confidence-building measures in the field of security of and in the use of ICTs will be **consistent with international law**".

The **OSCE Ministerial Council endorsed these confidence-building measures**[3] and encouraged OSCE participating States to contribute to the implementation of these.

[1] PC.DEC/1106: https://www.osce.org/pc/109168
[2] PC.DEC/1202: https://www.osce.org/pc/227281
[3] MC.DEC/5/16: https://www.osce.org/cio/288086

Organization for Security and Co-operation in Europe

Regional organizations such as the OSCE are ideal platforms for building confidence in cyberspace: They have often been conceived for conflict prevention, and offer practical expertise with CBMs and associated mechanisms that can be applied to this new domain. The OSCE is the first regional security organization with such a diverse constituency that has managed to reach agreement on cyber CBMs.

Implementation of OSCE CBMs

In recent years, the OSCE's work on cyber/ICT issues has **focused on the implementation of the OSCE cyber/ICT security CBMs.** Besides national implementation by individual states, the OSCE Secretariat has set up a number of cyber capacity-building projects aiming to assist participating States in this endeavour.

The activities range from tailored **implementation roadmaps** for a specific participating State and **workshops** for representatives of the OSCE sub-regions, to **enhancing the OSCE-wide implementation of CBMs** as well as **strengthening the OSCE Point of Contact network**.

Operationalizing the OSCE Point of Contact Network

The OSCE's efforts to implement the confidence-building measures on nominating national Points of Contact into a **crisis communication network** and as a **platform for co-operation** might serve as a good example to other regions and UN member states on how to operationalize CBMs. International co-operation as well as mitigation of eventual conflicts requires communication between parties, therefore establishing a **directory of policy (and technical) points of contacts** proved to be helpful. It must be stressed that the aim of this directory is not to duplicate already existing technical communities (e.g. FIRST, EU CSIRT network, etc.) but is considered serving as a regional risk reduction mechanism aimed at preventing conflicts stemming from the use of ICTs by States.

OSCE confidence-building measure No. 8 on Points of Contact reads as follows:

"*8. Participating States will nominate a contact point to facilitate pertinent communications and dialogue on security of and in the use of ICTs. Participating States will voluntarily provide contact data of existing official national structures that manage ICT-related incidents and co-ordinate responses to enable a direct dialogue and to facilitate interaction among responsible national bodies and experts. Participating States will update contact information annually and notify changes no later than thirty days after a change has occurred. Participating States will voluntarily establish measures to ensure rapid communication at policy levels of authority, to permit concerns to be raised at the national security level."*

The contact details of the policy and technical points of contact – as voluntarily announced by the participating States – are listed on a **closed online platform**, only accessible with a password. For the verification of availability of e-mail addresses, the OSCE Secretariat regularly conducts so-called **Communication Checks**. The first of such exercises merely aimed at checking the availability of the national points of contact by requesting them to answer via e-mail a simple question within a given timeframe, while the most recent Checks are not pre-announced to participating States and involve more complex tasks, often requiring national

co-ordination. The Communication Checks increasingly request direct interaction between two points of contact (and not merely the communication with the OSCE Secretariat), in line with the aim to further encourage co-operation between states.

As a next step on strengthening the Points of Contact Network, the OSCE Secretariat holds **annual meetings for the points of contact** aiming to further build trust and confidence between the experts. It also envisages to promote common understanding of cyber/ICT threats and to discuss co-operative actions that can meaningfully address them. Moreover, the OSCE Secretariat **facilitates bilateral meetings between individual points of contact** of different participating States with the aim to exchange best practices and build professional relationship promoting mutual co-operation in times of crisis.

Co-operation among regional organisations

The OSCE Secretariat welcomes the **increasing involvement of regional organisations into the UN processes** on cyber stability, and was honoured to have been the first organisation the Chair of the Group of Governmental Experts conducted regional consultations with. It also gladly accepted the invitation to share its experiences in the implementation of confidence-building Measures in the Open-ended Working Group.

At the UNIDIR-CSIS Workshop on "The Role of Regional Organisations in Strengthening Cybersecurity and Stability: Experiences and Opportunities" held in January 2019 the Director of the OSCE Transnational Threats Department emphasized the crucial role regional organisations play in enhancing international cyber stability, and suggested to bring these organisations together on a regular basis to facilitate exchange under the UNIDIR platform. This proposal was well received among participants of the workshop and it would be welcome **if the modalities on co-operation among regional organisations under the UN umbrella could be explored with the aim to regularly share experiences and exchange information.**